(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034687 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/NO02/00380

(22) International Filing Date: 21 October 2002 (21.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001 5093 19 October 2001 (19.10.2001) NO
60/330,089 19 October 2001 (19.10.2001) US

(71) Applicant *(for all designated States except US)*: **SECURE GROUP AS** [NO/NO]; P.O.Box 172, N-1325 Lysaker (NO).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HANSEN, Torgeir** [NO/NO]; Bisp. Nicolasgt. 6, N-0652 Oslo (NO). **GRUSD, Eystein** [NO/NO]; Vøyensvingen 5c, N-0458 Oslo (NO). **MEHLUM, Thomas** [NO/NO]; Nordahl Bruunsgt. 17, N-0165 Oslo (NO).

(74) Agent: **BRYN & AARFLOT AS**; P.O.Box 449 Sentrum, N-0104 Oslo (NO).

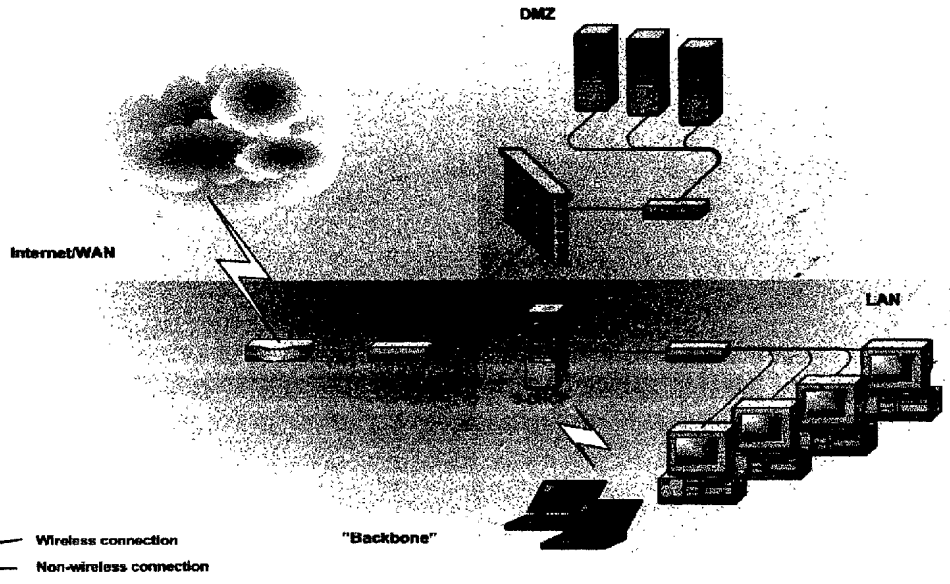
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR SECURING COMPUTER NETWORKS USING A DHCP SERVER WITH FIREWALL TECHNOLOGY



(57) Abstract: A method and system for securing computer networks from unauthorized access is described. The network comprises a DHCP server withfirewall technology, and authentication of a client requesting access to the network is performed on DHCP level by using a combination of the MAC address and IP address for the requesting client.Only clients with allowed combinations of the MAC and IP address are given access to the network through the DHCP server in a certain time period.

WO 03/034687 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and system for securing computer networks using a DHCP server with firewall technology

INTRODUCTION

The present invention relates to network communications, and in particular to a system and method for securing computer networks.

BACKGROUND

Today, computer networks are secured against hackers and other unauthorized access through various forms of firewall technology. Firewalls have become an important part of network design, as networks and servers contains valuable information which shall not be destroyed or otherwise tampered with in an unauthorized way. Also, a firewall provides secure access from a secure computer network to open networks, like the Internet.

In Figure 1, a network system, which is a combination of a secure and insecure network, is shown. The insecure part of the network is in Figure 1 constituted by an Internet or WAN (Wide Area Network) architecture and the secure part is a LAN (Local Area Network), a typical network in a corporation. The computers on the LAN side is protected by firewalls, controlling client machines requesting access to the LAN, and allowing communication and access to systems on the insecure network from the secure part of the network. The firewall includes an Internet Protocol (IP) layer. Present firewalls often have static protection of the IP/MAC (Media Access Control) address, and are therefore especially vulnerable for IP/MAC spoofing.

Also, the number of wireless networks is increasing, and subcontractors of these networks have not taken account of the fact that such networks are open to absolutely anyone if one is within a certain range. An example of a wireless network is shown in Figure 2 (flash).

DHCP (Dynamic Host Control Protocol) is today used in most networks. DHCP is a protocol for dynamically allocating IP-addresses to computers on a local area network. The system administrator assigns a range of IP addresses to DHCP, and each client on the LAN has TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period. The opportunities for unauthorized machines connecting to the network are large. A lap-top could e.g. be plugged into a

network contact nearly anywhere, be assigned IP-addresses and gain access to the network.

Networks may also be secured by a borderwall, and this technology will then only give access to certain IP-addresses. However, for an ill-natured hacker, or an employee, it is not much effort required accessing the unprotected parts of the network.

Also, virus creation kits, hostile chat software, network sniffer software, logical bombs, remote access tools, all compromise the network security from inside, and are seldom detected by any computer virus software. To be able to detect many of these programs you need to be a specialist in computer security with a wide knowledge of hacker software.

There is therefore a need for controlling and monitoring the network more carefully, than in the present methods.

SUMMARY OF THE INVENTION

The present invention is conceived to solve the security problem in open networks and provide better security in network solutions.

In accordance with a first aspect the invention provides a method for securing computer networks from unauthorized access, the network comprising a DHCP server with firewall technology. The method includes authenticating a machine requesting access to the network on DHCP level by using a combination of the MAC address and IP address for the requesting machine. If the machine has an allowed combination of the MAC and IP address, the firewall in the DHCP server is opened for traffic in a certain time period. However, if the combination of MAC and IP address does not exist, access is denied.

A description database on the DHCP server comprises combinations of MAC addresses and IP addresses that will give access to the network, and authentication is performed by comparing in a server processor the combination of the MAC address and IP address for the requesting machine with the allowed MAC and IP addresses in the description database. The authentication step first comprises comparing the MAC address of the requesting machine with the MAC addresses stored in the database, and if a match occurs, checking whether the machine has requested an IP, and if an IP has been requested, secondly compar-

ing the IP address with the IP addresses assigned to the MAC address stored in the database.

The server has the ability to monitor an insecure part of the network, providing overview of all clients in said network part requesting access to the network. Access for a new client machine to the network is given when adding the MAC and IP address pairs to a description database on the DHCP server. Withdraw of access allowance for a client machine to the network is achieved by deleting the MAC and IP address from a description database on the DHCP server. Network activity is monitored and data collected analyzed in an analyzer means.

The server/firewall and authentication is managed via an administrating interface. This is a web interface only available from a machine in a secure part of the network. Addition and deletion of MAC and IP addresses in the description database is then effectuated by a mouse-click.

In a second aspect the invention provides a system securing computer networks from unauthorized access, the network comprising a DHCP server with firewall technology. An administration interface in a client computer in a secure part of the network controls access to the network and controls both the DHCP server and firewall. Authenticating means authenticates clients requesting access to the network, and the authentication is performed on DHCP level by using a combination of the MAC and IP address for the client machine requesting access to the network. The administration interface also provides a log of activities on the network.

A program means may also be provided opening the firewall in the DHCP server for traffic in a certain time period, for the machine requesting access, for an allowed combination of MAC and IP address. An alarm means may be included forwarding an alarm signal to the administration interface creating a log and/or sending an SMS whenever unauthorized access is detected.

In a third aspect the invention provides a computer program product for a data processing system comprising a computer readable medium, having thereon a computer readable program means which, when loaded into an internal memory of a data processing system, makes the data processing system perform the method as outlined above. There is also provided a computer program product for a data processing system comprising computer readable code means which, when

loaded into an internal memory of a data processing system, makes the data processing system perform the inventive method.

The present invention provides a unique way of authenticating all users in a network, and also allows simple administration of users that shall have access, temporary or permanent, to the local network. In short, the present invention provides:

- a more secure wireless network.
- fully automatic installation of the product.
- ability of simple addition and deletion of users
- possibility for temporary users
- user authentication on DHCP level, both in wireless and cable networks
- cheap "burglar insurance"

All administration of the system is done through a web interface, simplifying the administration of both the DHCP server and the firewall. In known security tools, administration of normal DHCP servers and firewalls are separate products. In the present invention, one single interface controls both the DHCP server and the firewall. In prior art products the allowed MAC addresses had to be added manually to the database, and the configuration of the firewall and the editing of the text files belonging to the DHCP server performed in separate operations.

The present invention secures access to the network, and the assignment of IP-addresses. Both the MAC and IP address must have a matching pair in the DHCP database for gaining access to the network. A vast amount of MAC addresses exist, and it is almost impossible to guess a new MAC address. The invention is stated in the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

Embodiments of the present invention will now be described with reference to the drawings, which, as mere examples without limitations, show some designs related to this invention.

Figure 1 shows a computer network combination of a WAN/Internet and LAN network with known firewall architecture,

Figure 2 shows an network in which the present invention has been implemented, and

Figure 3 is a flow chart of the authentication procedure according to an embodiment of the invention.

DETAILED DESCRIPTION

The inventive security system may be implemented in e.g. a LAN (Local Area Network) architecture, as shown in Figure 2. In Figure 2 the LAN is connected to a WAN (Wide Area Network) or Internet. The network architecture may also be wireless as shown with the flash in Figure 2. The client computers in the LAN are not limited to personal computers or lap-tops, as pictured in the drawings but can be constituted by terminals, microprocessors etc. An administration interface is accessed from any one of the client computers in a secure part of the network, the LAN side in Figure 2.

The secure network in this context is defined as the network that is to be protected. Dependent on the configuration and/or location, the secure network is generally the network containing services that one wants to protect. Such services clients want protected are e.g. servers, access to local networks, Internet access etc. Even though Internet in itself is insecure, Internet is defined as secure when it is to be protected. Clients requesting authentication is defined as being on an insecure network. In Figure 2 the LAN is defined as secure, and the Internet/WAN as insecure. Clients requesting access to the LAN network in Figure 2 will be subject to the security system implemented in the S-DHCP server.

The security system comprises a modified and optimized DHCP server (S-DHCP in Figure 2) and an administration interface on one of the clients in the LAN in Figure 2. (The firewall in Figure 1 is replaced by the S-DHCP in Figure 2.) Access for a client requesting access to the secure network (LAN in Figure 2), by trying to connect to the network from e.g. the Internet side or through one of the clients on the LAN side of the network, e.g. a laptop within the range of a wireless network or login procedure from a terminal in a cable network, will be subject to an authentication procedure.

Authentication

The present invention authenticates the users on DHCP level by using the MAC (Media Access Control) addresses, and by using the combination of MAC and IP address. All network cards in client computers have a unique MAC address identifying the client in which the network card is installed. An example of a MAC address is: MAC: 00:50:56:01:00:00.

The modified DHCP server comprises a description database controlled by the administration interface. The description database contains information regarding the client machines having access to the network. The description database in the DHCP server holds information regarding the MAC addresses and the combinations of MAC and IP addresses having access to the network at the time a request for access is received by the DHCP server. Machines with MAC addresses not in the description database will be denied access. In the present system a specific IP address or addresses are assigned to each MAC number, and stored in the database. An example on such a combination is: MAC: 00:50:56:01:00:00, IP: 10.10.10.57. Only machines having the correct combination of MAC and IP address will gain access to the network.

The authentication procedure is illustrated in the flow chart in Figure 3. A client on the Internet side of the network trying to access the LAN (the case in Figure 2), will send a DHCP call together with an IP address to the S-DHCP server. A machine requesting access to a network will always try to be assigned the same IP address as in the last request. Accordingly, an IP address is also submitted to the S-DHCP server.

A S-DHCP server processor first checks whether the MAC address of the requesting client matches a MAC address in the server database. If the MAC address exists in the database, the next step in the authentication procedure is initiated. The server checks whether the client machine has requested an IP. If an IP has been requested, the server checks whether that MAC address has an assigned IP address in the server database. If the MAC and IP address pair exists in the database, the firewall is opened for that machine in a short time period. If the machine requests with a MAC/IP pair not in the database, the firewall is not ope-

ned, and access denied. Access is always denied and the next step is not initiated, if a step results in the answer "no" as shown in Figure 3.

S-DHCP server

The DHCP server in the present invention is configured in an optimal way, but is in other respects a normal DHCP server. This configuration is achieved with a standard DHCP server, but with specially designed applications, together providing the desired security aspects. In an embodiment of the invention a Linux based system is used. A DHCP Distribution server software from ISC (Internet Software Consortium) is then used as it is the de facto DHCP server standard in Unix/Linux machines. The ICS's DHCP Distribution software provides a freely redistributable reference implementation of all aspects of the DHCP protocol. (See also **http://www.isc.org/products/DHCP/** which is hereby included by reference.) The Linux software has also a built-in firewall functionality. The inventive DHCP server with Linux firewall and inventive software, functions as firewall between the two segments, i.e. a secure and insecure network as shown in Figure 2.

Specially designed software executes the authentication procedure outlined above. This software is stored in a memory on the S-DHCP server. The function of the applications executing the present invention as described above, will be listed in the following.

ipmac: monitors the "raw" network traffic logged by the S-DHCP server. The MAC address is embedded in the IP from a client and this logging, the MAC address can be identified. By this monitoring, all clients trying to connect to the network with unauthorized IP/MAC addresses will be detected. Ipmac then provides blocking of the S-DHCP Linux firewall for these clients on the network. This blocking is provided by an application ipclose. The ipmac requests information concerning authorized IP/MAC address pairs from the description database stored in a server memory.

ipclose: enable the firewall which blocks traffic from selected machines through the server web interface.

ipopen: opens traffic from selected machines through the server web interface.

newip: application used when the DHCP server configuration has been changed. The program runs the application makedhcpconf (will be described later), restarts the DHCP Distribution server software and instructs the ipmac application to re-read all the IP addresses and MAC addresses.

activecheck: application run regularly to check whether the authorized machines are actually on the secure network. If any of these machines are not logged on the network, the assigned IP address is blocked in the firewall on the DHCP server. When these machines are again detected on the network, they will then be subject to the authorization procedure, before given access to the network again.

makedhcp: program building the configuration files for the DHCPD server.

tracedhcp: a program tracking the DHCPD and detecting when a new client is requesting authentication. The application provides opening of the firewall to an extent enabling the authentication procedure to be performed for the client.

remipconfirm: application reading/writing to the DHCP description database containing the allowed IP and MAC addresses.

The administration tool with web interface in the secure network has two main functions: 1) adding authenticated IP/MAC addresses to the server database, and 2) providing a logging function when unauthorized access is detected. The network administrator uses the administration interface to control access to the secure network. The administration interface is a web interface providing a readily intuitive overview of all machines "seen" on the "insecure" network, and certain machines may then be given access to the "secure" network by e.g. a click of a mouse. By this action the IP/ MAC address pair is automatically added to the description database in the S-DHCP server. The database is then used as basis information for the application makedhcp, building a S-DHCP configuration file, containing information of authorized IP/MAC address pairs. The authenticated client machine will then be given access to the secure network. Also, a client computer that no longer shall have access to the network, may be deleted accordingly by a

mouse-click in the web administration interface. This causes the IP/MAC address pair for the client computer in question to be removed from the S-DHCP server database and then accordingly from the S-DHCP configuration file.

When a client computer requests access to the system with an IP address or a MAC address or a combination of a MAC and IP address that is not already held in the server database, the authentication system in the DHCP server sends an alarm via SMS and/or sends a message signal to the administration interface which creates a log of the incident.

The web interface provides easy management of the machines allowed on the secure network, and machines may easily be added or deleted by the click of a mouse. A message is then immediately sent to the description database in the fire-wall on the DHCP server, which is then updated. This also provides the possibility for temporary users.

The product may be delivered to the customer on a computer readable medium, e.g. a CD-ROM or floppy disk, , together with two network cards, that can be installed by the customer, on any of the client machines in the network to be protected, i.e. a network defined as secure. Any network can be protected, including Internet, WAN, customer network or LAN. The software itself may also be transferred via a network e.g. Internet. The installation interface is intuitive and easy to use and only demands that the user has IP addresses available, type of network card, and if any SCSI cards should be used in the machine from which installation is performed. Upon installation the DHCP server in the network to be protected is modified and optimized to provide the specified security function. After installation all network administration is performed through the web interface as explained above.

Having described specific embodiments of the invention it will be apparent to those skilled in the art that other embodiments incorporating the concepts may be used. These and other examples of the invention illustrated above are intended by way of example only and the actual scope of the invention is to be determined from the following claims.

CLAIMS

1. A method for securing computer networks from unauthorized access, the network comprising a DHCP server with firewall technology, the method comprising:
- authenticating a machine requesting access to the network on DHCP level by using a combination of the MAC address and IP address for the requesting machine, and
- if the machine has an allowed combination of the MAC and IP address, to open the firewall in the DHCP server for traffic in a certain time period,
- if the combination of MAC and IP address does not exist, access is denied.

2. Method according to claim 1, wherein the DHCP server comprising a description database comprising combinations of MAC addresses and IP addresses that will give access to the network, and authenticating by comparing the combination of the MAC address and IP address for the requesting machine with the allowed MAC and IP addresses in the description database.

3. Method according to claim 2, wherein the authentication step first comprises comparing the MAC address of the requesting machine with the MAC addresses stored in the database, and if a match occurs, checking whether the machine has requested an IP, and if an IP has been requested, secondly comparing the IP address with the IP addresses assigned to the MAC address stored in the database.

4. Method according to claim 1, comprising monitoring an insecure part of the network, providing overview of all client machines in said network part requesting access to the network.

5. Method according to claim 1, comprising giving access for a new client machine to the network by adding the MAC and IP address to a description database on the DHCP server.

6. Method according to claim 1, comprising removing the allowance of access for a client machine to the network by deleting the MAC and IP address from a description database on the DHCP server.

7. Method according to claim 1, comprising managing authentication via an administrating interface, the administration interface being a web interface only available on a machine in a secure part of the network.

8. Method according to claim 5 or 6, wherein the addition and deletion of MAC and IP addresses in the description database is performed by a mouse-click in the administration interface.

9. Method according to claim 1, comprising monitoring network activity and collecting data to be analyzed in an analyzer means.

10. A system securing computer networks from unauthorized access, the network comprising a DHCP server with firewall technology, the system comprising:
- an administration interface in a client in a secure part of the network, controlling access to the network and controlling both the DHCP server and firewall,
- authenticating means for authenticating a client machine requesting access to the network, the authentication being performed on DHCP level by using a combination of the MAC and IP address for the client machine requesting access to the network.

11. System according to claim 10, wherein the DHCP server comprising a description database holding information on combinations of MAC and IP addresses having access to the network.

12. System according to claim 10, wherein the administration interface provides a log of activities on the network.

13. System according to claim 10, wherein the authenticating means first checks whether the MAC address for the requesting machine exists in the description database, and if the MAC address exists, checks whether the requested IP address exists for the MAC address.

14. System according to claim 10, wherein the administration interface controls access to the network by adding or deleting MAC and IP address pairs to/from the description database, respectively.

15. System according to claim 10, comprising a program means opening the firewall in the DHCP server for traffic in a certain time period, for the machine requesting access, for an allowed combination of MAC and IP address.

16. System according to claim 10, comprising an alarm means forwarding an alarm signal to the administration interface creating a log and/or sending an SMS whenever unauthorized access is detected.

17. System according to claim 10, wherein the administration interface is a web interface.

18. System according to claim 10, wherein the network is a cable network.

19. System according to claim 10, wherein the network is a wireless network.

20. Computer program product for a data processing system comprising a computer readable medium, having thereon a computer readable program means which, when loaded into an internal memory of a data processing system, makes the data processing system perform the method in one of claims 1-9.

21. Computer program product for a data processing system comprising computer readable code means which, when loaded into an internal memory of a data processing system, makes the data processing system perform the method in one of claims 1-9.

Figure 1

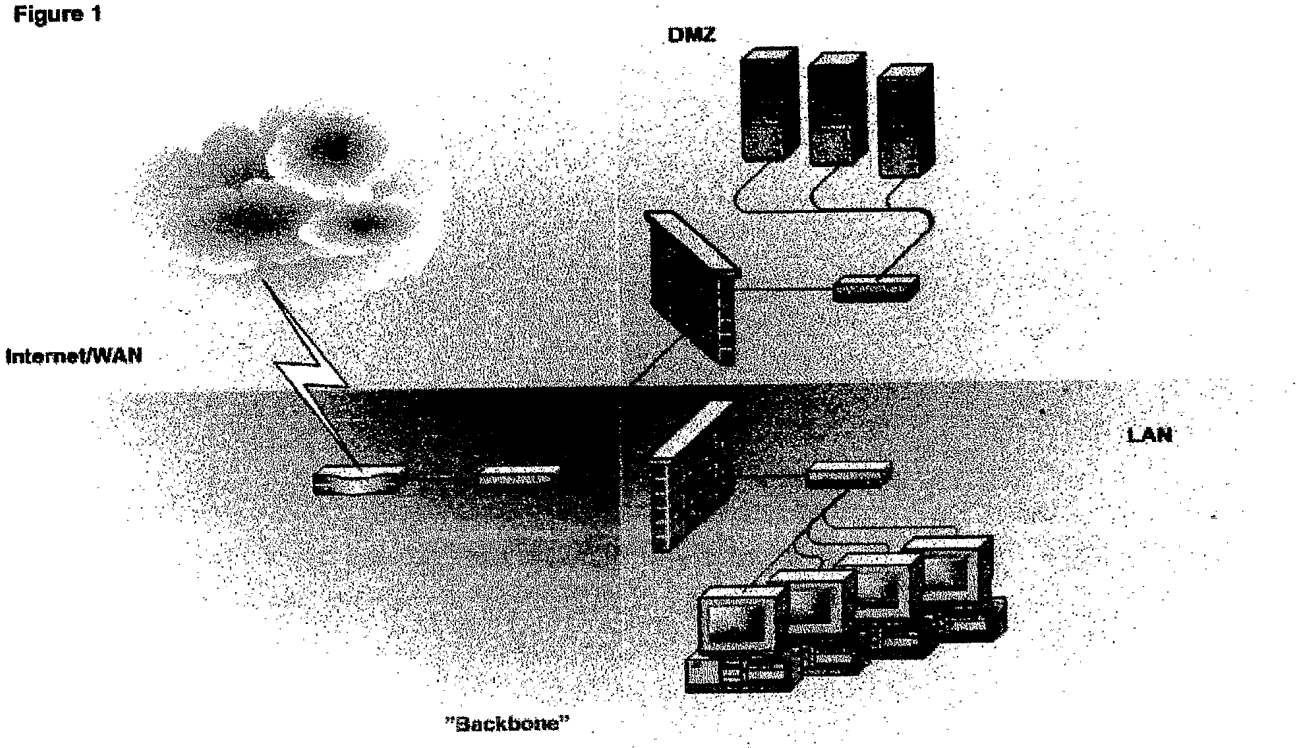


Figure 2

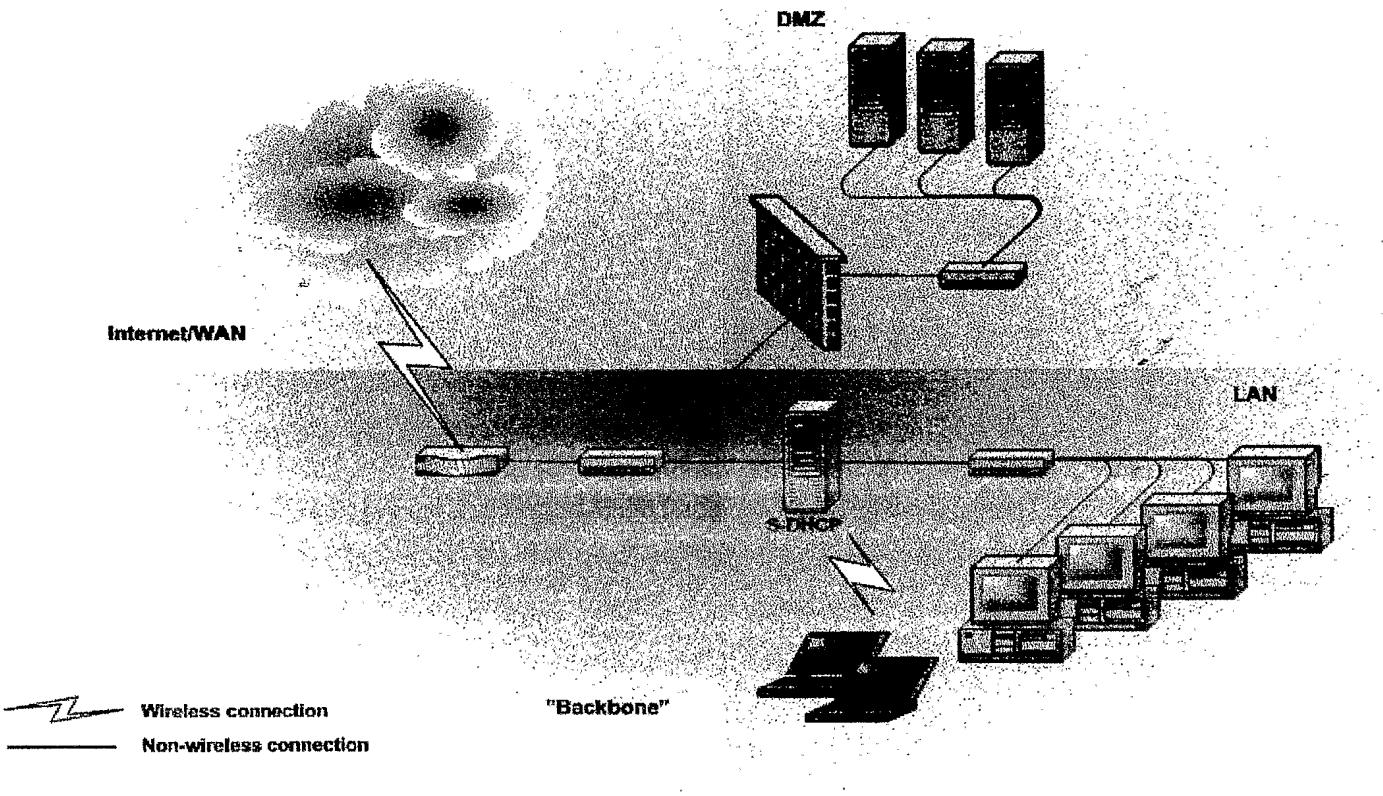
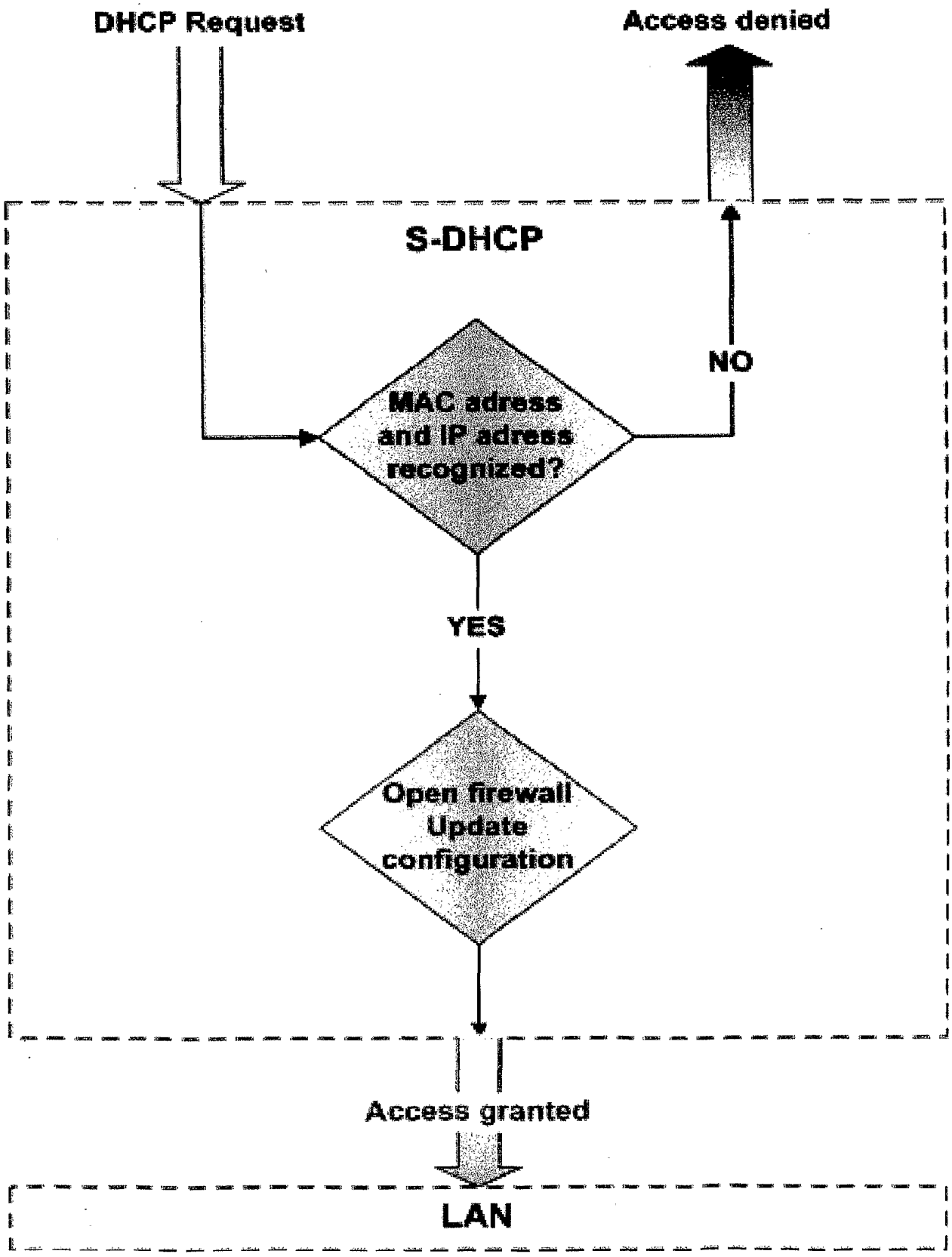

DMZ
Internet/WAN
LAN
"Backbone"
Wireless connection
Non-wireless connection

Figure 3


DHCP Request
Access denied
S-DHCP
NO
MAC adress and IP adress recognized?
YES
Open firewall Update configuration
Access granted
LAN

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 02/00380

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 29/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 0131843 A3 (NOMADIX, INC.), 3 May 2001 (03.05.01), page 4, line 6 - line 23; page 17, line 27 - page 18, line 6, claims 1,8,10, abstract ---	1-21
Y	PATENT ABSTRACT OF JAPAN JP 2001 211180 A, 2001-08-03 (3 Augusti 2001) NEC COMMUN SYST LTD abstract --- --------	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 January 2003	23-01-2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Ralf Boström/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/12/02

International application No.
PCT/NO 02/00380

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0131843 A3	03/05/01	AU 1224301 A	08/05/01
		AU 1340401 A	08/05/01
		AU 2297601 A	08/05/01
		AU 2614401 A	14/05/01
		EP 1222775 A	17/07/02
		EP 1222791 A	17/07/02
		EP 1224788 A	24/07/02
		WO 0131886 A	03/05/01
		WO 0131889 A	03/05/01
		WO 0133808 A	10/05/01
		AU 1224101 A	08/05/01
		WO 0131885 A	03/05/01
		AU 1224201 A	08/05/01
		EP 1232610 A	21/08/02
		WO 0131861 A	03/05/01
		AU 1098301 A	08/05/01
		EP 1226687 A	31/07/02
		WO 0131855 A	03/05/01
		AU 1088501 A	08/05/01
		EP 1234425 A	28/08/02
		WO 0131883 A	03/05/01

PUB-NO: WO003034687A1

DOCUMENT-IDENTIFIER: WO 3034687 A1

TITLE: METHOD AND SYSTEM FOR SECURING COMPUTER NETWORKS USING A DHCP SERVER WITH FIREWALL TECHNOLOGY

PUBN-DATE: April 24, 2003

INVENTOR-INFORMATION:

NAME	COUNTRY
HANSEN, TORGEIR	NO
GRUSD, EYSTEIN	NO
MEHLUM, THOMAS	NO

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SECURE GROUP AS	NO
HANSEN TORGEIR	NO
GRUSD EYSTEIN	NO
MEHLUM THOMAS	NO

APPL-NO: NO00200380

APPL-DATE: October 21, 2002

PRIORITY-DATA: NO20015093A (October 19, 2001) , US33008901P (October 19, 2001)

INT-CL (IPC): H04L029/06

EUR-CL (EPC): H04L029/06 , H04L029/06

ABSTRACT:

CHG DATE=20030603 STATUS=O>A method and system for securing computer networks from unauthorized access is described. The network comprises a DHCP server withfirewall technology, and authentication of a client requesting access to the network is performed on DHCP level by using a combination of the MAC address and IP address for the requesting client.Only clients with allowed combinations of the MAC and IP address are given access to the network through the DHCP server in a certain time period.